

# DIGITAL EVIDENCE AND COMPUTER CRIME

**FORENSIC SCIENCE, COMPUTERS AND THE INTERNET**

Second Edition

by Eoghan Casey

*with contributions from*

Robert Dunne  
Monique Mattei Ferraro  
Troy Larson  
Michael McGrath  
Gary Palmer  
Tessa Robinson  
Brent Turvey



**ELSEVIER**  
ACADEMIC  
PRESS

Amsterdam • Boston • Heidelberg • London • New York • Oxford  
Paris • San Diego • San Francisco • Singapore • Sydney • Tokyo

ACKNOWLEDGMENTS	vii
DETAILED TABLE OF CONTENTS	ix
AUTHOR BIOGRAPHIES	xvii
INTRODUCTION	1
<b>PART 1 DIGITAL INVESTIGATION</b>	<b>7</b>
CHAPTER 1 DIGITAL EVIDENCE AND COMPUTER CRIME	9
2 HISTORY AND TERMINOLOGY OF COMPUTER CRIME INVESTIGATION	25
3 TECHNOLOGY AND LAW	41
4 THE INVESTIGATIVE PROCESS	91
5 INVESTIGATIVE RECONSTRUCTION	115
6 <i>MODUS OPERANDI</i> , MOTIVE, and TECHNOLOGY	147
7 DIGITAL EVIDENCE IN THE COURTROOM	169
<b>PART 2 COMPUTERS</b>	<b>191</b>
CHAPTER 8 COMPUTER BASICS FOR DIGITAL INVESTIGATORS	193
9 APPLYING FORENSIC SCIENCE TO COMPUTERS	211
10 FORENSIC EXAMINATION OF WINDOWS SYSTEMS	255
11 FORENSIC EXAMINATION OF UNIX SYSTEMS	289
12 FORENSIC EXAMINATION OF MACINTOSH SYSTEMS	323
13 FORENSIC EXAMINATION OF HANDHELD DEVICES	337

<b>PART 3 NETWORKS</b>	357
CHAPTER 14 NETWORK BASICS FOR DIGITAL INVESTIGATORS	359
15 APPLYING FORENSIC SCIENCE TO NETWORKS	383
16 DIGITAL EVIDENCE ON PHYSICAL AND DATA-LINK LAYERS	419
17 DIGITAL EVIDENCE ON NETWORK AND TRANSPORT LAYERS	441
18 DIGITAL EVIDENCE ON THE INTERNET	477
<b>PART 4 INVESTIGATING COMPUTER CRIME</b>	519
CHAPTER 19 INVESTIGATING COMPUTER INTRUSIONS	521
20 SEX OFFENDERS ON THE INTERNET	561
21 INVESTIATIONS CYBERSTALKING	601
22 DIGITAL EVIDENCE AS ALIBI	617
<b>PART 5 GUIDELINES</b>	625
CHAPTER 23 HANDLING THE DIGITAL CRIME SCENE	627
24 DIGITAL EVIDENCE EXAMINATION GUIDELINES	633
BIBLIOGRAPHY	645
GLOSSARY	665
AUTHOR INDEX	675
SUBJECT INDEX	677